Submission in response to the National Health (Privacy) Rules 2018 review

Australian Privacy Foundation

4 June 2021

About the Australian Privacy Foundation and this submission

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. Information about the APF appears at the end of this submission.

The APF response to the Office of the Australian Information Commission's *National Health (Privacy) Rules 2018 review* (the Review) is outlined herein.[1] The APF has made previous submissions on these issues to the ACCC and the government in response to *the ACCC Digital Platforms Inquiry*, *the ACCC Customer Loyalty Schemes Review* and *the Attorney-General's Review of the Privacy Act 1988 (Cth) – Issues Paper*.[2-6] These responses inform this submission. It is also consistent with a range of detailed official and civil society analyses over the past few years, as detailed in those previous submissions.

The APF supports this review process because it may help to address what we have noted, a significant lack of engagement from federal health authorities when asked to respond to civil society inquiries on important and significant matters relating to personal information protection and health. These authorities include, but are not limited to, the Australian Digital Health Agency (ADHA), the Department of Health (DoH), the Australian Institute of Health and Welfare (AIHW) and the Therapeutic Goods Administration (TGA).

This APF response covers the key questions asked in the Review unless otherwise noted.

Part 1: Submission body

Key Review Questions

1 What provisions in the Rules work well and should remain as they are or with minimal changes?

2 What provisions in the Rules are no longer fit for purpose? Why?

3 Do the Rules get the balance right between protection of privacy on the one hand and use of claims information on the other? Why or why not?

With respect, this review is too vague as a meaningful discussion of the Rules, which remain a complex legislative instrument under section 135AA of the *National Health Act 1953.*[7] The Act and Rules, accompanied by supporting amendments, annexes and notes, comprise more than 500 A4 pages of complex reading, not to mention frequent and significant cross-referencing: a body of dense documentation demonstrating both that the Rules require simplification and that the review timeline is insufficient. Both of these problems need to be addressed before or alongside the questions above. Nonetheless, we offer initial feedback here.

The APF is of the view that provisions in the Rules do not work well for the Australian community, and require replacement. The opaque and complex matrix of responsibilities outlined in the Rules on the one hand, accompanied by the lack of consequences for misuse or misinterpretation by end-users (with limited or ineffective transparency and remedies for those affected by these flaws) on the other hand, is a persistent discomfort.

The discomfort endures because none of the Rules seem fit for purpose; it is unclear how to undertake accreditation of security and privacy controls. For example, the Rules are ambiguous, so we question how they are interpreted and implemented by the DoH. We understand the decision-making process DoH uses for the release of the PBS and MBS data relies on applications to the AIHW, its ethics committee and then advice to its own internal committee, the Data Access and Release Policy panel (DARP).[8] DARP guide the DoH delegate around PBS and MBS use and linkage.[(9)] This process lacks transparency, or a process for external oversight, or input by those affected, yet it may influence risks for every Australian. The AIHW data governance director and ethics secretariat might be excused if it were a little confused or unclear about what is needed. Further, there is no public record of decision-making. The advice of a professionally recognised privacy or security expert might provide useful support here, as would input or consultation with citizens, advocates, researchers and intermediaries in this area.

The Rules are one of several overlapping regulatory requirements, such as those bridging Australian Federal, State and Territorial jurisdictions, cancer databases, hospital information systems, and defence personnel and veterans' rules. Medical researchers are already able to store MBS and PBS numbers in the same database and link these to medical and health information, for example, in clinical trials and the Primary Health Insights (PHI) project.[10-12] The consistency of the Rules, and the ways they complement or otherwise affect other requirements, is a threshold issue that should be audited and laid out prior to review. A consistent legislative tool set is as important as its content.

An essential foundation for reviewing these Rules is that human rights are universal; a keystone is seeking and obtaining an individual's active, properly-informed consent.[13] Respect for and reliance on such active consent is applicable across the spectrum of sexual activity, legal jurisdictions, instruments and proceedings, research and medical practice but not, it seems, Australian health or medical information (beyond situations which may warrant exceptions, like public health emergencies). 'Patient-centred care' is often treated as simply jargon but it is not possible without obtaining the legal permission of participants. The Rules do not uphold this right currently.

The APF maintains the current Rules should be abandoned and replaced by a simpler more coherent legislative instrument that embodies internally and externally consistent, best practice data security and personal information protection arrangements that respect human agency, drawing on wider consultations with those affected, than the current review.

Section 2 of this feedback provides context and evidence supporting this position.

Part 2: Context and evidence

1. Introduction

The APF acknowledges ongoing researcher and policymaker desires to authorise data linkage projects in opposition to the desire of many Australians to protect the privacy of their sensitive, personal information in medical, health and clinical records. This tension is not new, manifested in an Australian Law Reform Commission (ALRC) report tabled in August 2008. The ALRC report recommended that privacy be recognised as a fundamental human right that "should take precedence over a range of countervailing interests, such as cost and convenience".[14] We confirm our commitment to the principles outlined in the ALRC report. We add our concerns that the sophisticated network of Australian medical and health databases stored locally and in "the cloud", combined with ongoing advances to technology in support of convenience and cost to governments and researchers, and a growing hostility to respect for the role of patient and public interests in relation to medical records protection, has disrupted and undermined consent processes and challenged the expertise of these end-users. The APF would be happy to help with developing responses to these issues.

2. Review question themes: separate storage, storage without identifiers, prescriptive vs principles-based data storage

As noted by the Australian National Audit Office (ANAO) in March 2020, the DoH was assessed in 2018-19 regarding implementation of best practice cybersecurity strategies.[15] Years later the DoH remains at the lowest possible ('ad hoc') maturity rating for its cybersecurity practice.

Changing the Rules to 'principles-based guidance' will not contribute to the needed uplift in Australian cybersecurity maturity to protect national health data assets such as the PBS and MBS information. In the absence of engagement with the question of active consent, the increasingly common failures of cybersecurity, or the factors driving risk with an emphasis on exploitation rather than protection, it is unclear how the more ambiguous, uncertain and compliance-compromised model of 'principles-based guidance' can avoid leading to a deterioration in practical and transparent privacy protection.

How DoH and National Data Commissioner (NDC) staff are qualified to undertake accreditation of secure cloud environments, or to implement the current Rules, is nebulous. The DoH DARP, which advises the Secretary on approval of current PBS and MBS linkage requests, provides extremely limited public information on decision-making rationales, and no public record of decision making at all.[9] The APF has requested information from the TGA, the DoH, the AIHW and ADHA about electronic health and medical record data holdings and applications this year. The requests are acknowledged digitally, but even when direct contact is made, for example to the AIHW, our response was delegated to the DoH and we have obtained no response.[(16)] Queries by civil society about these processes often seem to be met by silence.

Australian researchers and public health policy makers already have principles-based access to terabytes, possibly even petabytes, of sensitive patient care data via the current health ecosystem.[17] This includes the Multi-Agency Data Integration Project (MADIP) Research Projects (MADIP), controlled by the Australian Bureau of Statistics.[18] The MADIP brings together a range of micro datasets and aggregated data in a single portal from Veteran's Affairs, the Australian Taxation Office, Centrelink, identified Census questionnaires and other DoH (or Services Australia) information. Access to many of the datasets is only open to trained University researchers and Government agents and not to civil society more generally.[18]

Notably, the PHI project also maintains a knowledge system which holds both MBS and PBS data in the same database, where information is collected by data extraction applications fitted to general practice Computerised Information Systems (CISs) after ostensible de-identification. De-identified data can, increasingly, be re-identified (or have traits useful for re-identification revealed) by appropriately equipped foreign and domestic actors, researchers, and miscreants.[12, 19] This vulnerability to re-identification already exists, and while there is a reluctance and lack of seriousness in bringing this to public attention, it is likely to increase over time with the ongoing progress in advanced data analytics methods and the proliferation of other public and private data sets, both authorised and unauthorised.

A key de-identification technique here is the removal of only some direct identifiers, such as personal contact details. The removal of other potentially key identifiers, such as PBS and MBS numbers from a health record, seem to ensure compliance with legally accepted, Australian, de-identification practices. [20] The OAIC has offered advice about additional measures, but this seems to be overlooked in real life.[12, 21]

The Rules do not provide sufficient, detailed guidance on secure, de-identified data storage. They do not guide authorities on ways to deal with and disclose the constantly degrading level of protection likely to be provided by any particular digital method over time, nor the potential future importance of data minimisation as a response to this threat. The ways security and privacy requirements are prioritised generally remains obscure.

The Rules should either prescribe more detailed conditions which align with best practice cybersecurity requirements, guided by the Australian Signals Directorate (ASD), or an equally ranked security organisation, and by reference to the growing international body of knowledge on re-identification risk and auditing, or be entirely removed.

The General Practice information collection is evidently refreshed each time a patient consults their GP and is then sent on to one of 31 Primary Health Networks (PHNs) for storage, based on implied and bundled, passive consent mechanisms. Refer to Appendix 1 for illustrations of such generic consent mechanisms and an individual's attempt to withdraw implied consent from the secondary data collection on request.[12] The patient data collection, known as the PHI project by the DoH, is then supplied to the AIHW, upon application, for research and other public health management purposes.[22]

The Federal government has designated the AIHW as the national data custodian to aggregate, control, use, access, secure and control individual privacy of the PHI information and the *Practice Incentives Program- Quality Improvement* (PIP-QI) eligible datasets.[12, 23-24] Their capacity to adequately address the potential conflicts of various public, professional and individual interests in relation to privacy and data protection is unclear.

The DoH also has access to around 400 categories of medical information, including MBS and PBS identifiers, of up to 25 million individual patients' medical records via the PHI data extracted from general practitioner's records for each healthcare user treated. The PHI data collection, linked to the DoH, is in prima facie breach of both s. 135AA and the public's expectations that the data will be kept separate .[1, 23-24] The Rules must address this abuse of people's trust in their doctors and Australian health authorities.

This breach manifests the disruptive influence of technological advances on privacy controls, and informs the social determinants of health, the choices the public make about our health and the systems we put in place to protect ourselves and our loved ones. Public trust in Australian medical information systems and public health advice is diminishing as the application of digital technology in health outpaces the technical knowledge of end-users and the willingness to confront the implications of risks around declining data security and ongoing attacks on privacy.[25] Current shortages in Australian work force digital health expertise, as well as the worsening global shortage of cyber security expertise, amplifies these concerns.

The ADHA's My Health Record (MHR) system, an apparent centrepiece of data collected by health authorities, adds information to government health and medical knowledge collections of interest to third parties outside the clinical relationship but has minimal utility to the clinical relationship due to data integrity flaws. While it was redesigned when initial opt-in measures failed to gain the support and trust of patients, efforts were made to undermine opt-out consent. Nevertheless, around 10% of Australians have opted out of MHR, many due to privacy concerns.[26] The MHR system design suffers from functionality deficits, such as accurate and easily auditable authentication, identification, authorisation and Directory Services tasks, which have fostered adverse health outcomes.[27-28] The default user access model is also the opposite of data security best practice (and of the initial model of a 'Patient Controlled' electronic health record) and reason for public and clinical concern.

Publicly available, third party and independent assurance of the health and medical research environment assessment, added to an evaluation of cloud security appropriateness, including the

partitioning of sensitive data, encryption and anonymisation strategies, would advance public trust in the Australian health system.

The Rules do not, however, provide a sufficient level of detailed guidance on secure data storage and associated domains. Rule requirements need clarification as to the ways they are prioritised given alternative guidance, such as from the Commonwealth secure cloud strategy, the proposed New Distribution Category accreditation scheme, the Information Security Registered Assessors Program, Essential Eight and other ASD guidance.[29-32]

The sophisticated, highly connected Australian system of health databases can currently be linked 'on the fly' for many compliance related purposes too, including MBS and PBS claims audit information, supported by the *Health Legislation Amendment (Data-matching and Other Matters) Act 2019*, in concert with other, currently held, national information assets.[33] This was evidently demonstrated recently when the media claimed health data held by government authorities was matched with audit findings and used to deny quarterly PIP-QI payments to more than a thousand general practices.[34]

The evidence reveals no cause for the Rules to be amended to principles-based ones. Principles-based Rules have failed the public. Primary examples include PHI co-location of MBS and PBS identification numbers in information extracted from local general practice CISs. Other government authorities champion integrated data for availability to government and researchers, such as MADIP and the AIHW, via portals. Rules concerning the separation of MBS and PBS data bases must remain, be updated to identify and protect against the continually growing threat of re-identification, and be adequately enforced. The *National Health Privacy Rules 2018* need to remain prescriptive.

3. Medicare PINs; Changes in technology; Should linkage of MBS and PBS claims information be allowed in circumstances beyond those currently prescribed?

Medicare Personal Information Numbers (PINs) should not be used for linkage or other purposes beyond those currently prescribed. Rather, MBS and PBS linkage should rely on privacy-preserving data linkage approaches, such as bloom filters.[35] The DoH has previously, and continues to, sponsor data linkage of national health data assets using bloom filters, a cryptographic hashing method which provide useful privacy protection. Linkage keys should be anonymised and suitably encrypted using best practice algorithms, or other techniques, which offer protection against the constant erosion of protection from past de-identification or obfuscation methods. Medicare PIN linkage or its

expansion, as proposed in the Rules review, appears a retrograde step, going in exactly the wrong direction.

The secondary use of the MHR for research purposes (given its limited usefulness for clinical purposes due to low data integrity) may in some circumstances prove a worthwhile goal and in the public interest, once effectively anonymised and audited for application. However, despite the secondary use framework being published in 2018, health authorities, ADHA, DoH and AIHW, with tripartite responsibilities for the MHR secondary data use, have not yet articulated a secure storage and governance strategy for the use of this data, nor revealed their approach to regularly researching the risk of re-identification as techniques advance over time and undermine particular past practices.[36-37] We think regulatory guidance provided by the current Rules is inadequate for government decision makers to act upon reliably.

Further, anecdotal evidence from a reliable source alleges that a Privacy Impact Assessment (PIA) and ethics decision-making inquiry on a proposed linkage of the MHR to the PBS in 2018 was not published by the AIHW. There is public confusion about why information about decision-making by the AIHW ethics committee and DoH DARP regarding PBS data remains unavailable. It is unclear how, if at all, the current Rules are considered by the Secretary of Health in decision-making to authorise PBS and MBS data release. 'Bandaid-ing' the Rules via the *National Health (Privacy) Rules 2018* review is unlikely to prove helpful to anyone. Much more transparency, consultation and open-ness about risk is essential for future public consideration about trustworthiness.

In any case, Medicare PINs are currently being linked under a range of prescribed circumstances by Services Australia (SA)/DoH.[38-39] These PINs are also linked, both together and to 400 pieces of confidential information per person arising from consultation with one's GP in PHI databases, without public knowledge.[40-41] Evidently the current Rules permit sufficiently broad linkages to meet the needs of all key government and researcher agencies.

No provision to expand PIN linkages needs to be put in the Rules; rather privacy-preserving linkage should be prioritised and obligations to regularly monitor and address the implications of the constant improvement of re-identification threats.

4. Technological development

The pace of current and future technological development exacerbates current and future risks that the PBS and MBS claims information, linked to PINs or other identifiers, may be inappropriately accessed or disclosed, or exposed to the risk of 'function creep' (which can potentially both intrude on privacy and render earlier security and access control options unreliable). Data analysis and networking technology has advanced so as to easily bridge enclaves in government agencies, research design and public health policy formulation. There is no need to expand the risks this creates by defining technology rather than privacy enhancing standards in the Rules. Digital database tools have evolved over time, so keeping the information stored in a federation of databases is not problematic for authorised end-users to link, when necessary, utilising ethical, standards-based and rapidly advancing deep learning, artificial intelligence, data storage and similar tools. [42-44]

The evolution of digital health tools has been accompanied by a surge in peer-reviewed, community group and academic fostered policy suggestions about ethical and privacy-enhancing ways to use the tools. Emerging Privacy Enhancing Technologies (PETs) support the moves by some health authorities to enable relevant data sharing while protecting privacy and confidentiality. The discussion paper reviewing the Rules does not explore available and future tools in support of PETs. For instance, homomorphic encryption is a PET that encrypts information such that it does not need a secret key for computation, but requires the secret key for other uses by the information owner.[45-46] We think it is critical to 'future-proof' the Rules (or their more comprehensible successors) by taking advantage of and promoting the use of emerging PETs, rather than focus on spurious and outmoded de-identification processes, supported by an unsophisticated, old-fashioned PIN encryption tool as the accepted way to link health and medical information.

5. Disclosure of claims information for medical research.

The disclosure of MBS information for medical research is not very useful for addressing medical and health concerns, or indeed, very much at all. MBS and PBS data provide useful administrative information whereby only some MBS and PBS data fields capture patient conditions and treatments. PBS and MBS data fields tend to exclude clinical and patient information, such as dosage information or conditions diagnosed. And the lack of standardised and interoperable general practice CIS tools means data quality is often variable, incomplete, and flawed.[47]

The operation of the Rules will also need to balance necessary and existing mechanisms for ethical oversight, while managing the risk of further contributing to the duplication in governance and ethical responsibilities between Human Research Ethics Committees (HRECs) and data custodians. HRECs must always provide approval for the disclosure of claims for medical research purposes and their role must be clearly delineated from government data custodian decision-making, including the implementation of alternative regulations – such as the Rules.

The current *Data Availability and Transparency Act 2020* and explanatory materials indicate that the DoH will be empowered to share PBS and MBS data in certain circumstances, despite the current Rules. This occurs under a broadly permissive and vague test where *'… the sharing must be reasonably necessary to inform government policy, programs or service delivery, or be in support of research and development'*.[48] It's unclear how the Rules will interact with this new proposed legislation, which removes the obligation for the DoH as the custodian of the PBS and MBS data, to act in accordance with the *Privacy Act* and National Health and Medical Research Council (NHMRC) guidance. Security rules about storing patient health information are growing more fragmented over time, adding complexity to the ongoing 'wicked problem' of digital health technology development and usability.

6. Interaction with the APPs

The APF recently responded to the Attorney-General's *Review of the Privacy Act 1988 (Cth) – Issues Paper*.[4] There is no significant difference between our responses to that submission and our response to questions asked in this Review. Please refer to Section 3 in our submission for detailed information.[4]

Nonetheless, the opaque behemoth that is *the National Health (Privacy) Rules 2018* has fostered a confusing, outdated, and complex legislative web under section 135AA of the *National Health Act 1953.* The Rules do not comply with best practice cybersecurity or policy formulation protocols, and do not protect the privacy of Australian individuals. The Rules are often vague, and inconsistent with other legislative instruments. Consent processes are frequently passive, diffuse and difficult for individuals to manage. PBS and MBS data is routinely linked with other health information for medical research, and no AIHW or DoH decision-making outcomes are publicly available. This situation is worsened by, for example, reportage that the Victorian government plans to compile a database of patient details from private hospitals, general practitioners, mental health systems and

ambulance services without each patient's consent, announced in December 2020.[49] The APF maintains that all provisions in the Rules should be removed and replaced in light of the APPs and the growing threats to the trustworthiness of Australian medical and health data systems.

The need for transparency and open-ness, active consent, explicit notification measures, and emphasis on responding to increased information security threats is vital for the community trust required to develop pervasive and safe health data systems across Australia. The Rules require reframing, simplification, and redrafting.

7. References

1. Office of the Australian Information Commissioner (OAIC) . *The National Health (Privacy) Rules 2018 review,* 4 June 2021 https://www.oaic.gov.au/engage-with-us/consultations/national-health-privacy-rules-2018-review/consultation-paper-national-health-privacy-rules-2018-review/
2. Australian Privacy Foundation (APF) 'Regulation of digital platforms as part of economy-wide reforms to Australia's failed privacy laws Australian Privacy Foundation submission to the Australian Government on implementation of the ACCC's *Digital Platforms Inquiry—Final Report*' 10 September 2019 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341044
3. Australian Privacy Foundation (APF) *APF submission on ACCC draft report 'Digital Platforms: The Need to Restrict Surveillance Capitalism'*, 22 February 2019 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341044
4. Australian Competition and Consumer Commission (ACCC) *ACCC Digital Platforms Inquiry* https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry
5. Australian Competition and Consumer Commission (ACCC) *ACCC Customer loyalty schemes review* https://www.accc.gov.au/focus-areas/market-studies/customer-loyalty-schemes-review
6. Australian Privacy Foundation (APF). *Bringing Australia's Privacy Act up to international standards* (Submission in response to the *Privacy Act Review - Issues Paper*), 17 December 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3752152
7. Australian Government National Health Act 1953, *Federal Legislation*. 22 July 2020. https://www.legislation.gov.au/Details/C2017C00250
8. Australian Institute of Health & Welfare (AIHW) *Accessing government health and welfare data* https://www.aihw.gov.au/about-our-data/accessing-australian-government-data
9. Dept. of Health *Data Access and Release Panel.* 15 February 2018. https://www1.health.gov.au/internet/main/publishing.nsf/Content/Data-Access-Release-Policy
10. Australian Institute of Health & Welfare (AIHW). *Primary health care.* 23 July 2020. https://www.aihw.gov.au/reports/australias-health/primary-health-care
11. Australian Institute of Health & Welfare (AIHW). *Researcher Resources*. Available 19 May 2021. https://www.aihw.gov.au/our-services/data-linkage/researcher-resources
12. Fernando, J. (2021) *Federal Government quietly reward GPs for patient health data without getting informed consent*, March. Australian Privacy Foundation. https://privacy.org.au/wp-content/uploads/2021/04/MBGovtGPsPatientData-210401.pdf
13. United Nations. Article 12, *Universal Declaration of Human Rights*. 10 December 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights
14. Australian Law Reform Commission (ALRC) *For your information: Australian Privacy Law and Practice* (ALRC Report 108) (Report tabled August 2008) https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

15. Australian National Audit Office (ANAO) *Managing Health Provider Compliance.* 23 November 2020. https://www.anao.gov.au/work/performance-audit/managing-health-provider-compliance

16. Australian Privacy Foundation (APF). *Publications; Indexed by Date*. 20 May 2021. https://privacy.org.au/publications/by-date/

17. University of Delaware. *Examples of data volumes*. https://www.eecis.udel.edu/~amer/Table-Kilo-Mega-Giga---YottaBytes.html

18. Australian Bureau of Statistics (ABS) *Multi Agency Data Integration Project (MADIP) Research Projects*. https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP+Research+Projects

19. de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. & Blondel, V. D. Unique in the Crowd: The privacy bounds of human mobility. Nature, 3: 1376. 25 March 2013. https://www.nature.com/articles/srep01376.pdf

20. Office of the Australian Information Commissioner (OAIC) & CSIRO Data 61. *De-identification Decision Making Framework*. 18 September 2017. https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/

21. Office of the Australian Information Commissioner (OAIC) *De-Idenitifactioin and the Privacy Act*, 21 March 2018. https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

22. Australian Institute of Health & Welfare (AIHW). *Researcher Resources*. Available 19/05/21 https://www.aihw.gov.au/our-services/data-linkage/researcher-resources

23. Durham, P. *PHN Data Arrangements a Bit of a Mess,* 27 September 2019. Wild Health Summits. https://wildhealth.net.au/phn-data-arrangements-a-bit-of-a-mess/?utm_source=website&utm_medium=listings-search&utm_campaign=PHN%20Data%20Arrangements%20a%20Bit%20of%20a%20Mess

24. Central and Eastern Sydney PHN. Frequently Asked Questions: PIP QI and Data Sharing. November 2019. https://www.cesphn.com.au/

25. Ward, P.R., Rokkas, P. & Cenko, C. et *al.* A qualitative study of patient (dis)trust in public and private hospitals: the importance of choice and pragmatic acceptance for trust considerations in South Australia*. BMC Health Services Research*;15(1). https://doi.org/10.1186/s12913-015-0967-0

26. Kaus, C. More than 2.5 million people have opted out of My Health Record. *The Guardian*. 20 Feb 2019. https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record

27. Dunlevy, J. *My Health Record issues prevent patients from getting COVID vaccine. News Corp Australia Network.* March 27, 2021. https://thewest.com.au/news/my-health-record-issues-prevent-patients-from-getting-covid-vaccine-c-2448194

28. Walsh, L., Hemsley B., Allan M., et al. Assessing the information quality and usability of My Health Record within a health literacy framework: What's changed since 2016? *Health Information Management Journal*. 2021;50(1-2):13-25. doi:10.1177/1833358319864734

29. Digital Transformation Agency (DTA) *Commonwealth secure cloud strategy.* https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf

30. International Air Transport Association (IATA). *Guide to NDC Accreditation Capacity*. 12 November 2019. https://www.iata.org/contentassets/6de4dce5f38b45ce82b0db42acd23d1c/guide-ndc-registration-certification-program.pdf

31. Australian Signals Directorate (ASD). *Information Security Registered Assessors Program* (IRAP). Available 24 May 2021. https://www.cyber.gov.au/acsc/view-all-content/programs/irap

32. Australian Signals Directorate (ASD). Essential Eight Explained. Available 24 May 2021. https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained

33. Parliament of Australia. *Health Legislation Amendment (Data-matching and Other Matters) Act 2019.* 12 December 2019. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6441

34. Scholefield, A. More than 1000 GP practices denied PIP payment after 'data-matching' crackdown. *Australian Doctor* 3 May 2021 https://www.ausdoc.com.au/news/more-1000-gp-practices-denied-pip-payment-after-datamatching-crackdown

35. Nilsson, S. *Bloom filters explained*. YourBasic.org; February 2018. https://yourbasic.org/algorithms/bloom-filter/

36. Australian Digital Health Agency (ADHA). ADHA Digital Health Agency Corporate Pam 2020-2021 https://www.digitalhealth.gov.au/sites/default/files/2020-10/Australian%20Digital%20Health%20Agency%20Corporate%20Plan%202020-2021.pdf

37. Department of Health (DoH) Framework to guide the use of My Health Record System Data; May 2018. https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf

38. Cancer Research Economics Support Team (CREST) *Medicare Australia data for research: an introduction*. November 2015. https://www.uts.edu.au/sites/default/files/2019-04/crest-factsheet-medicare-australia.pdf

39. Sax Institute. *Working with MBS and PBS data*; 28 May, 2021. SaxInstitute https://www.saxinstitute.org.au/events/training/working-with-mbs-and-pbs-data/

40. PenCAT *CS's Cat 4 De-Identified Extract Data Dictionary*. PenCS, October 2019. Available 21 January 2021. www.pencs.com.au

41. Outcome Health. General guide to using POLAR' PHN SE Melbourne; Accounts and Logins, p.5; *POLAR Data*. https://outcomehealth.org.au/polar.aspx

42. Australian Privacy Foundation (APF). *Cloud computing.* 11 November 2009. https://privacy.org.au/policies/cloud-computing/

43. Cameron, L.M. IEEE S*ecurity & Privacy. Artificial Intelligence and Privacy: Navigation and the ethics of automation*; September 19 2018. https://publications.computer.org/security-and-privacy/2018/09/19/ai-and-the-ethics-of-automating-consent/ Sept 19, 2018

44. Lee, O. *Artificial Intelligence and Data Protection: How the GDPR regulates AI*. Hunton Andrews Kurth. Centre for Information Policy Leadership (CIPL). EU Project on accountable AI. March 2020 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf

45. *Homomorphic Encryption Standardisation*. https://homomorphicencryption.org/introduction/

46. Gov.UK. *Centre for Data Ethics and Innovation Blog*; 9 February 2021 https://cdei.blog.gov.uk/2021/02/09/privacy-enhancing-technologies-for-trustworthy-use-of-data

47. Youens, D., Moorin, R. & Harrison, A. et *al.* Using General Practice Clinical Information System data for research: the case in Australia. *International Journal of Population Data Science*. 2020;5(1). https://ijpds.org/article/view/1099

48. National Data Commissioner. *The Data Availability and Transparency Bill has been Introduced to the Australian Parliament*; Department of Prime Minister and Cabinet. https://www.datacommissioner.gov.au/

49. Cook, H. Planned database of Victorians' health information 'trashes privacy'. *The Age*, 5 December 2020. https://www.theage.com.au/national/victoria/planned-database-of-victorians-health-information-trashes-privacy-20201204-p56kpc.html

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, Committees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

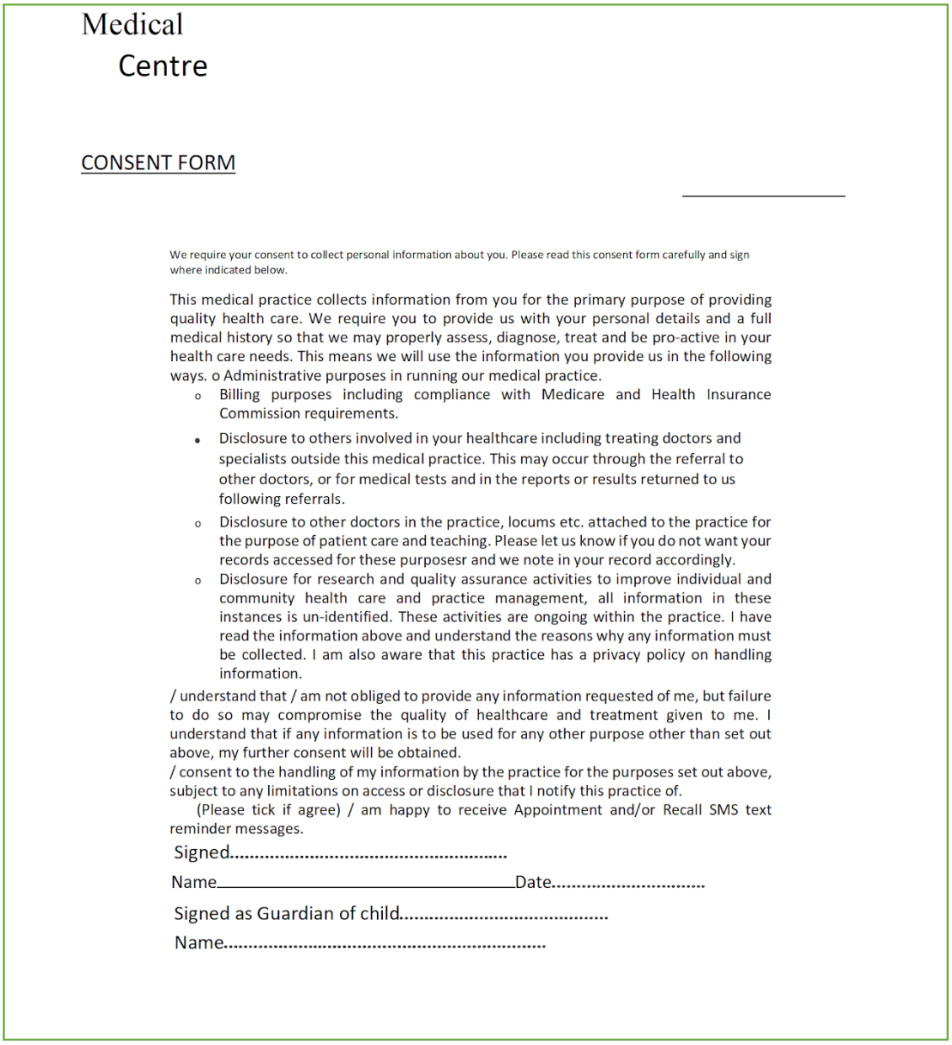
The following pages provide access to information about the APF:

- Policies https://privacy.org.au/publications/by-date/
- Media https://privacy.org.au/home/updates/
- Current Board Members https://privacy.org.au/about/contacts/
- Patron and Advisory Panel https://privacy.org.au/about/contacts/advisorypanel/

The following pages provide outlines of some of the campaigns that the APF has conducted:

- The Australia Card (1985-87) https://privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) https://privacy.org.au/campaigns/consumer-credit-reporting/
- The Census (2006) https://privacy.org.au/campaigns/census2006/
- The Access Card (2006-07) https://privacy.org.au/campaigns/id-cards/hsac/
- The Media (2007-) https://privacy.org.au/campaigns/privacy-media/
- The MyHR (2012-) https://privacy.org.au/campaigns/myhr/
- The Census (2016) https://privacy.org.au/campaigns/census2016/

Appendix 1



Medical
Centre

CONSENT FORM

We require your consent to collect personal information about you. Please read this consent form carefully and sign where indicated below.

This medical practice collects information from you for the primary purpose of providing quality health care. We require you to provide us with your personal details and a full medical history so that we may properly assess, diagnose, treat and be pro-active in your health care needs. This means we will use the information you provide us in the following ways. o Administrative purposes in running our medical practice.

- o Billing purposes including compliance with Medicare and Health Insurance Commission requirements.
- Disclosure to others involved in your healthcare including treating doctors and specialists outside this medical practice. This may occur through the referral to other doctors, or for medical tests and in the reports or results returned to us following referrals.
- o Disclosure to other doctors in the practice, locums etc. attached to the practice for the purpose of patient care and teaching. Please let us know if you do not want your records accessed for these purposesr and we note in your record accordingly.
- o Disclosure for research and quality assurance activities to improve individual and community health care and practice management, all information in these instances is un-identified. These activities are ongoing within the practice. I have read the information above and understand the reasons why any information must be collected. I am also aware that this practice has a privacy policy on handling information.

/ understand that / am not obliged to provide any information requested of me, but failure to do so may compromise the quality of healthcare and treatment given to me. I understand that if any information is to be used for any other purpose other than set out above, my further consent will be obtained.
/ consent to the handling of my information by the practice for the purposes set out above, subject to any limitations on access or disclosure that I notify this practice of.
(Please tick if agree) / am happy to receive Appointment and/or Recall SMS text reminder messages.

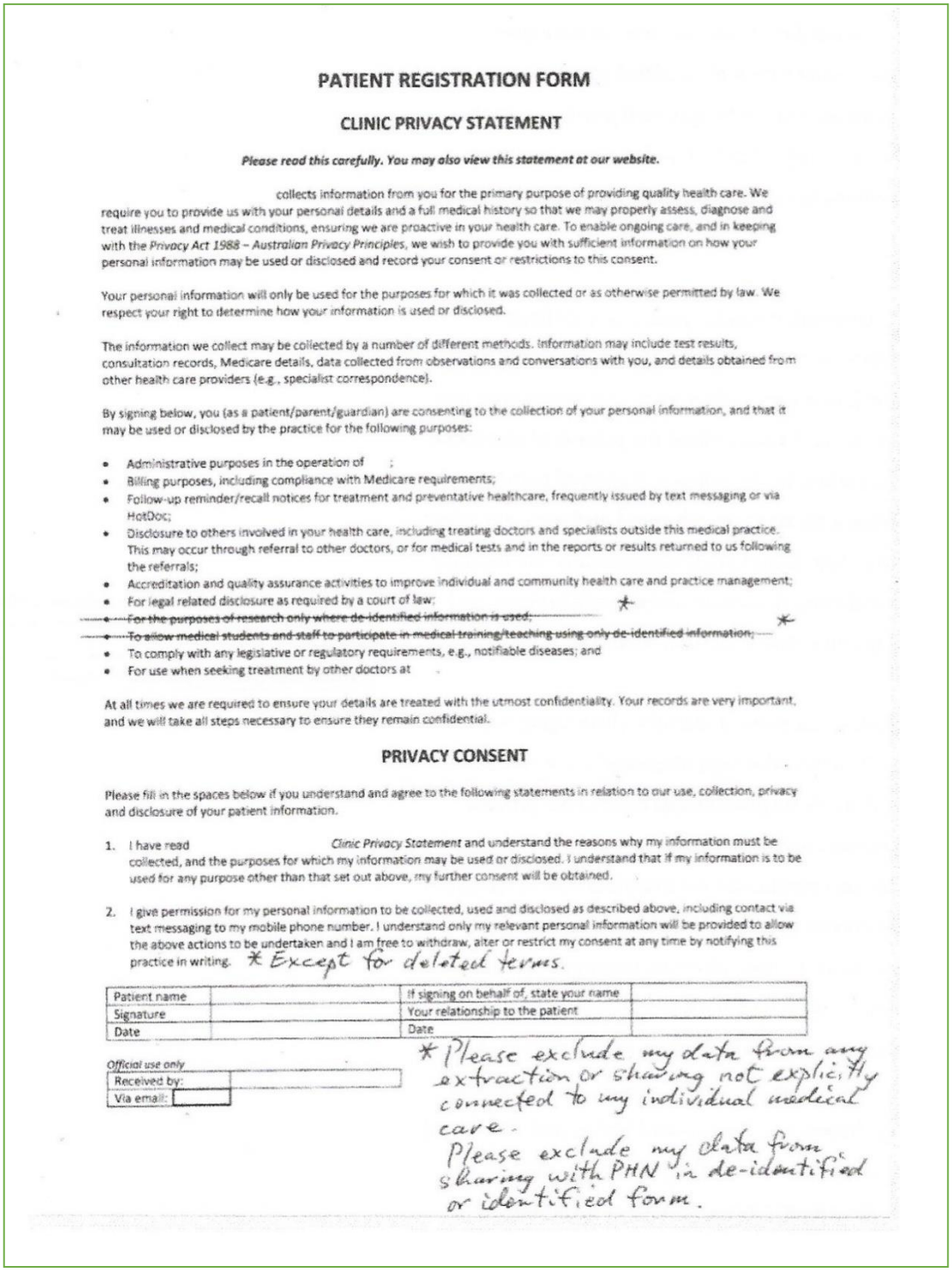
Signed.....

Name_____Date.....

Signed as Guardian of child.....

Name.....

Figure 1: Sample Medical Practice Consent Form



PATIENT REGISTRATION FORM

CLINIC PRIVACY STATEMENT

Please read this carefully. You may also view this statement at our website.

collects information from you for the primary purpose of providing quality health care. We require you to provide us with your personal details and a full medical history so that we may properly assess, diagnose and treat illnesses and medical conditions, ensuring we are proactive in your health care. To enable ongoing care, and in keeping with the *Privacy Act 1988 – Australian Privacy Principles*, we wish to provide you with sufficient information on how your personal information may be used or disclosed and record your consent or restrictions to this consent.

Your personal information will only be used for the purposes for which it was collected or as otherwise permitted by law. We respect your right to determine how your information is used or disclosed.

The information we collect may be collected by a number of different methods. Information may include test results, consultation records, Medicare details, data collected from observations and conversations with you, and details obtained from other health care providers (e.g., specialist correspondence).

By signing below, you (as a patient/parent/guardian) are consenting to the collection of your personal information, and that it may be used or disclosed by the practice for the following purposes:

- Administrative purposes in the operation of ;
- Billing purposes, including compliance with Medicare requirements;
- Follow-up reminder/recall notices for treatment and preventative healthcare, frequently issued by text messaging or via HotDoc;
- Disclosure to others involved in your health care, including treating doctors and specialists outside this medical practice. This may occur through referral to other doctors, or for medical tests and in the reports or results returned to us following the referrals;
- Accreditation and quality assurance activities to improve individual and community health care and practice management;
- For legal related disclosure as required by a court of law; *
- ~~For the purposes of research only where de-identified information is used;~~ *
- ~~To allow medical students and staff to participate in medical training/teaching using only de-identified information;~~
- To comply with any legislative or regulatory requirements, e.g., notifiable diseases; and
- For use when seeking treatment by other doctors at

At all times we are required to ensure your details are treated with the utmost confidentiality. Your records are very important, and we will take all steps necessary to ensure they remain confidential.

PRIVACY CONSENT

Please fill in the spaces below if you understand and agree to the following statements in relation to our use, collection, privacy and disclosure of your patient information.

1. I have read *Clinic Privacy Statement* and understand the reasons why my information must be collected, and the purposes for which my information may be used or disclosed. I understand that if my information is to be used for any purpose other than that set out above, my further consent will be obtained.

2. I give permission for my personal information to be collected, used and disclosed as described above, including contact via text messaging to my mobile phone number. I understand only my relevant personal information will be provided to allow the above actions to be undertaken and I am free to withdraw, alter or restrict my consent at any time by notifying this practice in writing. * Except for deleted terms.

Patient name		If signing on behalf of, state your name	
Signature		Your relationship to the patient	
Date		Date	

Official use only

Received by:	
Via email:	

* Please exclude my data from any extraction or sharing not explicitly connected to my individual medical care.
Please exclude my data from sharing with PHN in de-identified or identified form.

Figure 2: Practice consent form populated to withdraw from all secondary health data collection

Tue, 23 Feb 2021 at 17:25
>snip<
On another matter, would you please remove me from the PHN data collection application using PenCAT or POLAR, again as soon as convenient as I do not consent to the process.
Thank you

On Fri, 26 Feb 2021
14:24, wrote:
Hi there
Please confirm that you have removed me from the PHN data collection application using PenCAT or POLAR, for the PHN and PIP - QI data collection process/es as soon as possible as I do not consent to the process. See email below for my initial request last week. Any data you collect about me must only be shared for the purpose of primary health care; I do not consent to any secondary data collection.
Thanks

On Fri, 5 Mar 2021 at 11:19, wrote:
Dear Practice Manager,
Please confirm that you have removed me from the PHN data collection application using PenCAT or POLAR, for the PHN and PIP - QI data collection process/es as soon as possible because I do not consent to the process. See emails below for my initial requests - over 2 weeks. Any data you collect about me must only be shared for the purpose of primary health care; I do not consent to any secondary data collection.
On a related note, please email me a copy of the practice privacy policy.
Yours sincerely

09/03/2021
Dear Practice Manager
In hopes of speeding my enquiry re the practice privacy policy and my withdrawal of consent for my health information to be shared with PHN data collection and PIP-QI links, I went to your web site to download your new patient information sheet and consent paperwork but the link is dead, no file opens when I select that option.
Further, have you progressed my withdrawal of consent and would you confirm this. This discussion has continued for some time and I do not wish to take it to the Health Services Commission. Please respond to me.
Thank you

Figure 3: Individual's attempt to withdraw implied consent from a GP